



Home-based Working in the UK Committee

Corrected oral evidence

Monday 23 June 2025

3.15 pm

[Watch the meeting](#)

Members present: Baroness Scott of Needham Market (The Chair); Lord Farmer; Baroness Featherstone; Lord Fink; Baroness Freeman of Steventon; Lord Fuller; Baroness Manzoor; Lord Monks; Baroness Nye; Lord Parker of Minsmere; Lord Stevenson of Balmacara; Baroness Watkins of Tavistock.

Evidence Session No. 22

Heard in Public

Questions 223 - 230

Witnesses

I: Dr Ioannis Agrafiotis, Senior Cybersecurity Researcher, University of Oxford; Ryan Tanna, Founder, Blinktime; Chris Parker MBE, Director, Government Strategy, Fortinet.

Examination of witnesses

Dr Ioannis Agrafiotis, Ryan Tanna and Chris Parker.

Q223 **The Chair:** Good afternoon, everybody, and welcome to this second panel of the House of Lords Select Committee on Home-based Working. We are joined by three witnesses this afternoon. Thank you very much for coming to join us. This session is being broadcast live. You will receive a transcript to check for accuracy, and please feel free to send any supplementary evidence if there is something you think of later. The first question is from Lord Monks.

Lord Monks: We have heard a lot about the need for better management of people working from home on a hybrid or full-time basis, but I am particularly interested in how the three of you do it, rather than a general exhortation to do so. How did you get to the stage that you are at? I am particularly interested, Mr Tanna, in how you built up the company that you have developed, with a management software system that looks pretty detailed and controlling, if you want it to be. Perhaps you do not want it to be—I do not know—but could you tell us a bit about how it works? After that, I would be interested in your colleagues' comments on what you say.

Ryan Tanna: Thank you very much. I am the founder of Blinktime, which is a UK-based software start-up helping companies manage flexible working. It is embedded into daily tools so people can use it very easily to co-ordinate when they go to the office, where they are working from, and, crucially, who else will be in the office when they decide to go in. This helps with collaboration, reduces commuter regret and helps companies make better decisions with the data that they are able to gather. I will address the point about controlling, because that is quite an important aspect of how a tool such as Blinktime is adopted and received. Our clients include UK start-ups and some mid-sized businesses. As I said, we are a start-up, so we are very much in our early, learning stage, and taking feedback constantly from our different clients.

I founded Blinktime because I noticed a disorganised approach to flexible working and management, not just across different businesses but within businesses, across different line managers and departments. Having worked in a partnership before, I had witnessed almost a franchise-like difference between cultures in an individual department within a company. I also saw the experiences my wife had as an employee in a large corporate, and her interpretation of different policies and rules in how she manages and how her manager manages her. I thought there was a gap in the market for a standardisation or tool that reduced the ambiguity of what it meant to work flexibly.

The tool is primarily to aid employees rather than to be a Big Brother, let us say, for employers. It is useful for employers because they receive anonymous data on work patterns and can then create incentives to better tailor how they facilitate employees' work and how they make decisions about office utilisation and office space.

To address directly your question about how companies manage it, frankly, not very well. They tend to implement policy and rely on education internally, which leaves huge openness for interpretation and the overlaying of prejudices. That is not necessarily right or wrong; it is just the effect of only using a policy. Companies might be intentionally ambiguous on certain aspects of it, giving guidance and saying, “At the manager’s discretion”, which allows even more openness to interpretation and leads to concern among employees that they will be judged if they do something different from other people.

A lot of it is done on spreadsheets or by informal conversation with colleagues. A lack of being able to plan creates real frustration for employees, because they do not know when is best to go into the office, even though they know they have to because the policy directs them to. You then end up with people coming in and regretting doing so because everyone they would have worked with that day is at home. That was a long way of saying that it is not great.

Lord Monks: Could you give us an indication of the scale of the work that your company is doing? Obviously, there are other companies in the same field that have been brought to our attention. Are people using consultants in this area?

Ryan Tanna: They are definitely using consultants; whether they are using software like ours is difficult to know. As I said, we are still very early in our lifespan. We have a few hundred users across various sectors. Consultants are one of our go-to-market routes because companies are struggling to know how to manage and implement flexible working effectively and do not know that tech is available. They go to what they already do, which is to hire consultants to tell them how to better write policy.

Lord Monks: I would be interested to hear what Chris and Ioannis have to say about this.

Chris Parker: Thank you very much for inviting me here today. I am the director of government strategy at Fortinet, which is one of the largest cybersecurity companies in the world. Certainly, our view is not like Ryan’s; it is based solely on safety and security and keeping the data moving around safely and securely. From our point of view—I am sure we will explore it a bit more today—it is about making sure that people are aware that there are various factors in remote working, as you are no doubt aware. Technology is at such a level now that it is not a technological problem or a safety and security problem; it is about how you set it up and what you are using to do it. That is very positive news. As I hope to share later on, if people are interested, it is relatively low cost as well.

On the question of how to do it better and make it more procedurally correct, we have Ryan and his expertise, but on how to do things safely and securely, I can assure everyone that there is no difference at all

between remote working and working in an office, as long as—again, there are caveats—things are done properly and correctly.

Dr Ioannis Agrafiotis: Thank you very much for the opportunity to be here. I am a senior researcher at the University of Oxford's department of computer science and at the Global Cyber Security Capacity Centre. I have also been working at the European Union Agency for Cybersecurity, known as ENISA, for the past six years. I have about 15 years' experience in cybersecurity, so, like Chris's, my perspective will be from a cybersecurity point of view.

Over the past three or four years we have been conducting research on how working from home may impact the cybersecurity posture of users and organisations. We can go into details later, if you would like, about the data that we have at our disposal and the evidence that we have found, but I agree with Chris that Covid-19 was like a natural experiment in working from home, and it helped a lot in addressing cybersecurity issues, technology wise. We are definitely now in a much better position to work from home than we were five or six years ago.

Q224 **Lord Parker of Minsmere:** I should say at the start that I worked with Ciaran Martin for years—sorry about that. As you have both offered to, Chris and Ioannis, could you draw out the current cybersecurity risks for organisations that are quite mature in doing hybrid working, compared with how they might have worked pre-Covid? How are the cybersecurity risks and challenges different, and how are those organisations coping?

Dr Ioannis Agrafiotis: We surveyed about 4,500 people about two years ago, and the main research question was: did users experience more cybersecurity issues during or after the Covid pandemic, and did those relate to working from home or being in the office? Surprisingly, no matter what kind of statistical analysis we ran, the data suggested that users experience more cybersecurity problems if they change their location of working, independently of whether they work from home or the office. For example, if someone worked from home and then moved to the office, they experienced more cybersecurity issues than someone who was continuously working from home.

That might make sense, because you do not change your work habits, introduce new technology or introduce new software that you did not use before. We also asked questions like, "Did you experience more cybersecurity issues after the pandemic and after you moved back to the office?". The answer was, "Not necessarily, no", so I think we are in a much better position now. The risks that we could see before the pandemic were associated with risks that you would see in ordinary cybersecurity of organisations, like phishing emails, vulnerabilities in software, and so on. There were some risks associated with working from home technology only, for example remote desk protocols, VPN servers or video conference tools that did not used to be secure. But nowadays, I think most of these issues have been fixed.

Chris Parker: I agree with what Dr Ioannis has said and add that the whole world has now had to realise that cybersecurity challenges are in whatever you are doing, whether that be remote working, office working or anything. Primarily, of course, we remember that the bad actors involved are largely after either money or IP. There is some activism and things going on, but the big global worry is about ransomware—people trying to take data and do those things.

There is always a misconception that people at home are more relaxed, and therefore they can be more at risk and more likely to click on things. I would personally challenge that. I think we do not take risks with our fire safety or other safety. These things should become second nature to a digital generation, which we all have to now become, whichever our year of birth was. So, there are some combination factors there, and it is not just a function of the threat being out there, it is a constant chase of technology. The good news is there is extensive collaboration, both internationally and between the companies involved, to make sure everyone is safe—society, data and devices. But also, the big challenge now is how we educate people; maybe there is a need for some regulations and guidelines. We are very well served in this country with the UK National Cyber Security Centre, which has some excellent guidance: whether people follow it is always the challenge.

To summarise, I agree with what Dr Ioannis said: the real risks out there today are surmountable. They can be dealt with, and they will always be able to be dealt with. But again, people have to make sure they are set up in the right way to deal with it. It is like anything: your car safety, your fire safety and health and safety.

Lord Parker of Minsmere: We take your point that, at the macro level, being completely reductive about it, it is not materially different in terms of the overall quantum of risk because of the nature of the risk that is out there. If I just peel it back a little bit, it would be good to expose this as mythology if it is. I think the reason why some people—not experts—might believe there is more risk attached is that if a large proportion of your workforce is using their home PC as their workstation, it therefore sits outside the corporate protection of your IT department, which has locked down lots of functionality and is managing the device from the physical space it is in. Is that true or not? Is there more risk from people using their own devices more in hybrid working?

Chris Parker: It is an excellent question, and it is the nub of everything which is the myth or reality of homeworking. The hard reality is that the risks are there if people do not have the right technology and set-up to work at home. What is called the BYOD—bring your own device—era is now here, so people can use their own phone and load up their own work emails, for example. Some of you may do that yourselves, and people in the public will be well aware of us all doing that. Where the difference comes is that in the last five years or so, there have been huge advances in business, especially enterprise-level security on systems.

So, to log in and have those systems working on your own device means you are effectively a huge extension of the enterprise security. Therefore, it does not really matter as long as you have got the right thing set up where you work. It could be at home or on the train on your own device. Those systems allow checking and alerting and, more importantly, are updating all the time.

If we think back to an era I can remember well, we used to—a decade or two ago—buy some sort of antivirus in the early days and load it up every year. Those days have long gone because now we are into an era where you effectively buy a licence and things are constantly updating.

Now, digitally working from home, we must have the right configuration, the right set-up and the right behaviours—because we must remember a lot of this is about asking members of the public to be human firewalls, as we call it, and to be really alert and trained. We will get there. We need to make sure that we balance those three things: the technology, the set-up and people's behaviours.

Q225 Baroness Manzoor: Very briefly, what if people are not in the home, where they have the VPN set up and so forth? If they want to work from Pret, let us say, or in Italy, if they have gone on holiday but are partly working, does the same apply? Or is it that those systems are pertinent just to their home?

Chris Parker: Again, that is a very good question and you are quite right to ask it. A lot of people think, because they have heard the stories, that if you log in on a certain wifi, you might be at risk. Again, if you are using your normal system, looking at your family emails, as some people may well be doing, they have very good systems now, as do our mobile phones, and all those systems are built in. But if you are on an enterprise grade, so Fortinet's customers in government perhaps, or in large businesses—and small businesses, because it is the same technology—those enterprise systems reach right through that and it will be unaffected. The encryption will be unaffected by whatever wifi you are logging into, because the system will sort out and, more importantly, detect and deal with any issues involved. That is the removal of a myth: connectivity is not something to be cautious about, as long as you have the right technology and the right set-up and people are behaving properly.

Dr Ioannis Agrafiotis: I will add that there is a changed paradigm in cybersecurity and what is best practice at the moment. It used to be perimeter-first and you focus on the perimeter. Now, you may have heard the term "zero trust"; basically, you go from, "I have a perimeter" to "I don't trust anything". The idea is to go back to the devices that people may use, whether it is their own device or it is managed by the organisations, and you set up the devices in such a way that you make them secure, no matter where they are. There is this paradigm shift that has happened and it favours working from home.

Q226 Lord Parker of Minsmere: Could you both give us your impression or

knowledge—it may be slightly impressionistic—of where we are today in terms of the maturity of the implementation of the cybersecurity standards you are talking about, across the hybrid working environment that our economy now is? Where are we with that combination of human factors, skills training, the right tools and enterprise management? Where do you think we are at? Is there a gap or are we caught up?

Chris Parker: If there is a gap, it is simply in awareness and understanding of this. We will get there as long as we all understand what things have to happen. If you are running a small business, you just need to not think it is the responsibility of someone in IT and it is nothing to do with you. You just need to have a little bit of knowledge about the rules of thumb and the things that are involved. What I mean by that is that the technology is there and the costs are really quite low, so a small business might buy something which is about the same cost as its air conditioning equipment or its photocopier, and then be paying licence costs of something like £400 a year. We are really not talking about prohibitive costs to make sure that they are at the same standard of technology.

Certainly, in Fortinet, and other vendors would agree, to have the same engine size, you can go right up to a government department or an international military network, but it is the same technology. You can access it and you can pay for it and, as the previous panel mentioned, it is really about having the right people and protecting those people with the training levels, and the salary levels, to make sure they can stay with it. Having the people who can set up these amazing automated systems that keep us safe is the most important bit. If there is a gap, it is the awareness—perhaps among leadership and management levels—about how important that is and to make sure they are aware of it, because everything else is pretty much there in the market already. It is not a cost prohibitor or a technology prohibitor.

Dr Ioannis Agrafiotis: I totally agree that education and training are really important. One finding in our survey that was really surprising was that the majority of organisations had implemented more than 80% of the controls that we had as basic hygiene, and the user said they were cybersecurity aware. We had one question: do you share your own device with members of the family?

A massive amount of them replied “yes”. That begs the question, “You have all these cybersecurity controls in place, and you then trust your child with your computer, which may end up anywhere on the web?” So I definitely think that training is of paramount importance.

As a global cybersecurity capacity centre, we have a couple of maturity models. One is for nations; the other is for organisations. We have been to several nations. We see that many SMEs really struggle, especially those that are not part of the critical infrastructure. If there is no regulator in the sector to impose cybersecurity controls, they really tend to struggle. They may not even have guidance.

I do not have evidence for the UK, because the last time we did a study here in the UK was almost 10 years ago; I am sure that the UK has massively improved. I know that the UK is probably one of the pioneering countries in cybersecurity, but a lot of European countries and other developing countries—in Africa and Asia, for example—are really struggling with following basic cybersecurity hygiene. So any advice and models that the Government can provide to these organisations on how to set up their configurations and how to make decisions that are important to their security architecture will be of paramount importance.

Q227 Lord Fink: I have a question which may be out of pure naivety. As somebody who is plural in my employment, I have somebody at home—from a very reputable firm that I have dealt with for years—who basically comes on to my computer and takes it over to fix things and analyse things. I do not know what software they could be putting on there or what they could be copying from there. I probably go in once every couple of months to the IT services here in the House of Lords, and it is probably fair to say that I have never seen the same face twice. They use a series of contractors, with people coming in. How can we really trust cybersecurity on these sorts of systems when we have so many other agents, all of whom we have to trust, getting full access to our devices?

Dr Ioannis Agrafiotis: That is an excellent question. Insider threat is potentially one of the biggest threats that we see in organisations, so having the right systems in place to be able to detect it is of paramount importance, but it is important to focus on standardising services that you can get and, of course, on certifying people with the right skills. For example, CREST has an exceptional programme on penetration testing; there are requirements for critical services around what type of penetration testing people can access. If you create the standards and the certificates for the skilled people, you can be much more confident that whoever is delivering the service has some kind of standard and quality.

Chris Parker: I will add that there is some more good news. Whether you are in physical security or IT security, the vetting of staff is obviously really important, and any organisation, be it in the public or the private sector, will look at the people who hold the keys. The good news is that the technology industry, and Fortinet and others have been leading on this, has systems available to those who need it which allow them to spot anomalous behaviour and abnormal conditions; for example, people looking at files they should not be, in simple terms. There is an ability not only to do that but to deceive—people are doing that as well—which allows the follow-up and the law-and-order investigation. Those things are available on the market.

If you have a particular specialist need—we are talking about the high-risk sectors; again, as director of government strategy, I deal with a lot of our government space—you can be well served by that technology, because it allows us to back up the fact that there is even less risk of someone being able to do those things. However, there is still a big

weakness, always, in those who hold the keys, so it is, again, an employment and a trust piece.

I have one last thing to say about the thing that Dr Ioannis mentioned, zero trust. The systems involved there require multifactor authentication—some of you will use it every day, others less so—but, again, with certain systems, you can set up certain files so that you have to have facial recognition or a thumbprint recognition on your phone to create a token. Those systems are becoming pretty standard now; even dentists and doctors are using them routinely to protect our data. So, I think that the technology is now starting to wash through the market to make sure that the gaps that were there are being closed. Even if there is a live risk, because someone could be turned or blackmailed to do something, it would be very hard for them to be successful now.

Lord Fink: With hybrid working, as compared to fully remote working, do you see huge productivity gaps? If you think that there is a gap, how can we improve the difference between office working, hybrid and remote?

Ryan Tanna: Thank you for your question. Just to clarify, is your question about the difference between fully remote and hybrid?

Lord Fink: Yes; that is probably the most important one, because most jobs have gone hybrid now, I think.

Ryan Tanna: It is very difficult to measure productivity in certain industries, but some roles are easier than others. You can track sales, for example, based on some obvious metrics. I know that you have heard from Professor Nick Bloom, who has done a lot of research on this and has all the statistics.

We know from speaking to our clients, as well as the hundreds of HR and operations directors we speak to, that they find that some of the challenges with remote work are a real lack of collaboration, and loneliness creeping in for workers. So, although it can initially seem attractive, the shine wears off, and hybrid seems to be the sweet spot that people prefer. They find that hybrid employees are 45% more likely to say that they are more productive than their fully remote counterparts. They want to be in the office on some days, where they are more productive, when they are collaborating, then at home when they are doing deep work.

Where software can help with that is allowing people to be able to plan that to be most effective. They know that they are more productive in certain environments, but they do not know how to choose when they are going to be in those environments. It is about being able to predict that, to plan and to co-ordinate with their colleagues. Let us say that I will go in on Tuesday next week because the colleagues with whom I am working on a project are going to be in the office. I can maximise my productivity then; I will then do all my deep work on a Wednesday when they are not going to be in, so I will stay at home. Hybrid really is the sweet spot.

Remote companies can be very successful—I know founders of fully remote companies that are thriving and growing—but they tend to hire people across different countries and geographies. It works very well for their model but, for the vast majority, hybrid seems to be the blend that works.

Chris Parker: I can add something on that from personal experience. I am very lucky, in one of my volunteer roles, to be the vice-chair of techUK's Cyber Resilience Committee. We discuss these things and I can honestly say that, in my almost three years on that committee, I have never heard people say that one size fits all. The key skill here is part of modern management; we have it in our own company because we like to make sure of it. Certainly, from a Fortinet point of view, you would be a very foolish employer if you did not try to balance the needs of the workforce and its productivity in a sensible way.

My last point is that, if it is not to do with safety in technology and other issues, if we can get maximum productivity and avoid two or three hours' travel—as it sometimes is for me, as a leader and a manager—that is a really good use of people's time. However, we sometimes need to get some brainstorming and get some human factors going. Then, it is a different ask. In a high-tech, digital industry, we have a lot of people who need to work remotely. I should add that a lot of them really like it and enjoy home working; it gives them a lot of balance back as well.

Q228 **Lord Fuller:** Over the last few weeks and months, we have heard a lot about how we expect that the workplace and the way in which people interact from home will change as we look forward, but can we just focus on some of the technical landscape? We have heard about perimeter security, right down to zero trust. Is that something you see extending? What is remote working going to look like, at a technological level, in three or five years' time? Is it going to be easier or harder than it is now?

Chris Parker: It is a really good question. The simple answer is that technology will always stay ahead of the threat, because we will soon know if it does not. We are very well placed in the cybersecurity community globally: as I mentioned earlier, we share an awful lot. It is the most collaborative industry I have worked in by a long way—and I have worked in multiple sectors—because of the amount of need for collaboration.

Going forward, the technology will be there and will evolve. The threat may well evolve, but we are already seeing the early stages of that, and Fortinet's threat report and other threat reports have noticed a big uplift in the automation of the threat. Therefore, what is coming at us is now using a high degree of AI-leveraging automation. Interestingly, it is not necessarily producing some amazing new threat which is tying everyone in knots, it is just making the existing threats really difficult to spot, such as social engineering—emails and the use of those type of things. I think the evolution will be more in a ground where people are competing and making sure we are defeating those systems where people are using automation and AI.

The good news—there is lots of good news—is that companies such as Fortinet have been using very high grades of AI for about 10 years. It is just not something that, until now, has really been coming out, so the technology lead must remain there and there is literally billions of pounds in R&D going into it in the next period you are talking about. Because so much of the global economy is rooted in the need for this, I do not see cybersecurity falling behind the pace. It just cannot, because there is so much investment and real-time awareness of where this threat is moving. It is very unlikely that we get surprises these days: there is normally a real indication that something has evolved. It is very unusual to have a complete surprise.

Dr Ioannis Agrafiotis: I am really glad that Chris mentioned AI—I guess that this word must have cropped up in most of your meetings. In three to five years, technological changes with AI are going to have a huge impact. We already see this, for example, when you give full access to AI systems that are zero-click exploits: basically, you send an email to an organisation and then you are hacked. Organisations need to tread very carefully when implementing AI solutions to facilitate productivity and maybe solutions for working from home.

The good news, as Chris said, is that we seem to have aligned best practice with cybersecurity solutions for working from home. But any other technological solutions that are going to be invented in the next three to five years with a focus on working from home—for example, more collaborative environments, the use of different technologies to provide whiteboards with some tools to arrange meetings and so on—will need to be carefully evaluated for any kind of cybersecurity weaknesses.

Ryan Tanna: As a population, we tend to overestimate technological advancement in the short term and underestimate it in the longer term, so three to five years is a very interesting timeframe to look at.

As a non-cyber professional, there are certain things that I will want to do in person to guarantee that I am not a victim of fraud. I think that we will become more events-based in the way we work and there will be AI tools that help us, and maybe nudge us and say, “This looks like an event that might be better in person. These people are going to be in your area, maybe go and talk about bank details or whatever in person” and that kind of thing. Technology will leap in terms of experience for online and remote working, so it will be much easier to be able to collaborate, brainstorm and come up with creative ideas—things that people currently think are more difficult to do remotely. Where do I land? Again, back at hybrid working. Maybe it will be not so focused as it is today on the particular days that you are in, but on what you are doing.

Lord Fuller: I am slightly concerned about the security landscape for the small and medium-sized businesses. The PLCs and Government will look after themselves. I just wonder how we are going to have to upskill those small and medium-sized businesses to defend against these. Is it almost going to be a structural vulnerability among the businesses that do not have huge, dedicated IT departments? Will that have an effect on the UK

economy?

Chris Parker: That is a really good question. It is something that vexes us all. Before I was at Fortinet, I was a small business owner myself, and I know exactly what hard work it is and therefore there is very little time to say, "I will just go off on a course" or something. I think it is back to culture and awareness, and people have to now see that, going forward, there is no choice. You will just have to make sure that you have that hour a month to train. I use the word "training" rather than "education", because we are quite used to doing fire training, health and safety training or medical training in the workplace. We have to now ask our society to make sure we are doing this.

We, the cybersecurity companies, are not sitting back: Fortinet offer free training to the world, and it is highly successful. People use it and click on it and other companies offer training as well. NCSC has great training as well, but it is about getting people to do it. It is coming back to leadership, management and perhaps compulsion in the workforce. If I leave you with one thought, even in Fortinet, our people have to train for about three or four hours a month, sometimes more—I certainly have to—to keep up with the evolving technology. If we are doing that in the industry, and people outside are perhaps just doing nothing to a few hours a year, there is a gap, which was mentioned earlier. That is one of the gaps we can really try to close, with that compulsion to make sure people are trained in what to do.

Ryan Tanna: I will just add that as a small business owner, I am seeing that potential gap being closed by the private sector, or attempts at it. For example, our insurance requires us to do certain training, and provides free cyber training for all our employees that I then have to sign off that they have completed. Particularly, as a B2B business, my clients require certain standards to be held, and to have proof and certification, so we have an annual audit each year for that. Even as a very small business, we have access to those tools and are required to prove that we are adhering to them for the supplier requirements of our clients.

Dr Ioannis Agrafiotis: I definitely agree with Lord Fuller that we may see systemic risks with new technologies coming in in the next three to five years. The Government are in a unique position to run simulations, identify what these bottlenecks may be and come up with solutions. NCSC is an exceptional institution; it is pioneering. Years ago, it came up with the Cyber Essentials scheme. I was a naive researcher back then, and I thought, "Why are they proposing five or six basic cybersecurity controls that every cybersecurity expert knows?", but it was aiming at SMEs. If the Government can propose similar schemes and standards, that could potentially lead and pave the way for SMEs to secure their systems better.

Q229 **Baroness Featherstone:** How do various employer policies on home-working impact your organisations and what are the implications for your use of technology? We could perhaps start with Ryan.

Ryan Tanna: Perhaps it is easiest for me to answer this from our clients' perspective, because we talk to a lot of HR professionals about the policies that they have in place. It goes back to my response to the first question: they tend to be very ambiguous and open to interpretation. That means that you have the potential for line manager bias, perceived unfairness across different teams and different demographics. It may be comparable to the old smoker/non-smoker comparison. "If I do not have children or I do have children, why am I allowed different flexibility to the other group?".

Companies with better and more structured policies tend to have a higher employee satisfaction and are able to attract top-talent candidates more easily. Where they have structure or ways to implement it, perhaps through software, they are able to then measure it so that they can get the data and prove it to candidates when they are recruiting, instead of "flex-washing", which is saying what they know the candidates want to hear, and then when they arrive on day one, the successful candidate finds out that what was said on the website or in the job description is not really the situation in the team. If organisations can evidence it better, candidates can trust that what they are hearing is true, and they can invest in the right tools because they have the data to make those business cases internally. Policy varies, and the more structured it is, the better.

Baroness Featherstone: Do you find that your staff make comparisons between your company and other companies? Do they look at that?

Ryan Tanna: Absolutely. They sometimes care more about how many days they have to be in the office than they do about a bonus structure or pension contributions.

Baroness Featherstone: That is really interesting. Dr Ioannis, what is your finding on this?

Dr Ioannis Agrafiotis: I am afraid I do not have much to add on this topic. Our research is mainly focused on cybersecurity, but, speaking from personal experience, both at the university and ENISA, where I used to work, they were offering flexible regimes, so there was a clear policy. They had to slightly change the way that they came up with the metrics, so that the metrics and the policy were more project-oriented and caring more about collaboration. There were interesting problems with career progressions for people and how you monitor those.

When you have more flexible regimes, you tend not to have such great organisational culture, so they had things in place to make sure that the organisational culture was there. When you are onboarding new colleagues in an organisation, you need to have a mechanism in place, and all this would be part of the policy. Apart from that personal experience, I do not have anything substantial to add, such as evidence-based research, unfortunately.

Baroness Featherstone: That is okay, it is not an exam. Chris, I

understand you need to speak more broadly than about your own role in the office and about wider employment practices.

Chris Parker: Yes. The best comment I can add to that and to what Ryan said is that, from my point of view, it is about the impact on the organisation, which is what your excellent question was about. We have to try to help organisations have things easier, not more burdensome.

I checked this morning to make sure that I was factually correct about the cost for a small business of enabling perhaps 50 remote users to use the absolute gold standard latest level, which is Secure Access Service Edge. Again, that is Fortinet's model, which is now in the market with a lot of companies. Basically, everything you are doing goes through the cloud, gets completely secured and then goes off to do whatever you want it to do, or back again. Whatever you do badly, it will get found out, caught and sorted. It is the gold standard of what is available today for an organisation. The per-user cost for 50 users—again, it is based on licensing, because that is what happens there—works out at about £110 a year, so we are talking really low costs.

This is good news. Because of the prevalence in the market, costs that used to be quite high in IT and security are now quite low. As a citizen, I believe that is really good for small organisations, shops, schools and dentists. The costs are quite low rather than being prohibitive. What I would also like to see in the market, which we have discussed on the Cyber Resilience Committee and which was suggested in the McPartland review published before the change of government, is tax incentives for people who are buying cybersecurity to allow for some sort of tax benefit to small businesses, because that would further incentivise. The industry thought that that was a really innovative, sensible way of doing things. It could at least start a culture change—it may be time limited. That is something that is out there in a public review which may help the impact on organisations, but the cost is not, to my mind, prohibitive.

Baroness Featherstone: No. I was surprised when you said it was £110. Thank you.

Q230 **The Chair:** That leads us on to the last question. If each of you could make one recommendation to the Government in the area of home working, what would it be?

Ryan Tanna: From my perspective, it would be to see hybrid and flexible working in general not as a HR issue but as an economic productivity and infrastructure issue, and therefore to conduct UK inquiries and studies into the socioeconomic impacts of hybrid working that go beyond the productivity of companies and look at how it impacts birth rates, use of the NHS, the general health of the population, social mobility and so on. I think the implications of hybrid working can be far further reaching than just the productivity of individual companies, for which it is net neutral, anyway.

Chris Parker: Very simply, it would be to make sure that there is some end state that we can get to, by whatever means, of far greater increased awareness of what this is all about, rather than it being something quite mystical in the corner done by an IT department. We need something to bring it into the mainstream—a comprehensive training and education compulsion that makes sure that people realise, just as we have done with seat belts and other things in the past in our great country, that this is not optional. Let us all do it together and become more aware.

Dr Ioannis Agrafiotis: A few months ago, we published a framework, with the World Economic Forum, which we called a “compass”, for organisations to understand cyber resilience. The Government are in a unique position to do something similar for working from home. If we could create a framework—a compass—for SMEs and larger organisations to guide them on how they make decisions, not necessarily only on their policy on working from home but from governance and auditing all the way to more technical levels, that would be fantastic to see.

The Chair: Thank you very much indeed to you all for coming along to speak to the Committee. We greatly appreciate it.